EE512: Error Control Coding

Solution for Assignment on Cyclic Codes

March 22, 2007

1. A cyclic code, C, is an ideal genarated by its minimal degree polynomial, $g(x)$.

$$\begin{aligned} C &= < g(x) >, \\ &= \{m(x)g(x) : m(x) \text{ is a message polynomial of degree } \leq k\}. \end{aligned}$$

   We write the given code in polynomial notation with the basis $\{1, x, x^2, x^3\}$,

$$\begin{aligned} C(x) &= \{0, x + x^3, 1 + x^2, 1 + x + x^2 + x^3\}, \\ &= \{0, x(1 + x^2), 1 + x^2, (1 + x)(1 + x^2)\}, \\ &= < 1 + x^2 > . \end{aligned}$$

2. $\underline{c} = [0011010]$. In polynomial form,

$$c(x) = x^2 + x^3 + x^5 = m(x)g(x)$$

   for some $m(x)$. Since $g(x)|(x^n + 1)$, we notice that both $c(x)$ and $(x^n + 1)$ have $g(x)$ as a common factor. To get the smallest possible cyclic code, we need a $g(x)$ of largest possible degree. So we let

$$\begin{aligned} g(x) &= \gcd(x^n + 1, c(x)), \\ &= \gcd(x^7 + 1, x^2 + x^3 + x^5). \end{aligned}$$

   Euclid's algorithm:

   (a) Let us assume we want to find the GCD of the polynomials $a(x)$ and $b(x)$ where $\deg(a(x)) \geq \deg(b(x))$.
   (b) Let $r_{-1}(x) = a(x)$, $r_0(x) = b(x)$.
   (c) If $r_{i-1}(x) \neq 0$, divide $r_{i-2}(x)$ by $r_{i-1}(x)$ to get remainder $r_i(x)$ i.e. $r_{i-2}(x) = q_i(x)r_{i-1}(x) + r_i(x)$ with $\deg(r_i(x)) < \deg(r_{i-1}(x))$.
   (d) Repeat until $r_i(x) = 0$. If $r_i(x) = 0$, then $r_{i-1}(x) = \gcd(a(x), b(x))$.

   GCD of $x^7 + 1$ and $x^2 + x^3 + x^5$ is found using Euclid's algorithm as follows:

$$\begin{aligned} x^7 + 1 &= (x^2 + 1)(x^5 + x^3 + x^2) + (x^4 + x^3 + x^2 + 1), \\ x^5 + x^3 + x^2 &= (x + 1)(x^4 + x^3 + x^2 + 1) + (x^3 + x + 1), \\ x^4 + x^3 + x^2 + 1 &= (x + 1)(x^3 + x + 1) + 0. \end{aligned}$$

   Therefore, $g(x) = \gcd(x^7 - 1, x^2 + x^3 + x^5) = x^3 + x + 1$. The smallest cyclic code contain $\underline{c}$ is $C =< x^3 + x + 1 >$.

3. One generator matrix of a (n, k) cyclic code with generator polynomial $g(x) = g_o + g_1x + \cdots + g_rx^r$ $(r = n - k)$ is as follows:

$$\mathbf{G} = \begin{bmatrix} g_0 & g_1 & \ldots & g_r & 0 & 0 & \ldots & 0 \\ 0 & g_0 & \ldots & g_{r-1} & g_r & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & g_0 & g_1 & g_2 & \ldots & g_r \end{bmatrix}$$

Claim: There exists a generator matrix such that columns $\{j+1, j+2, \cdots, \jmath+k\} \mod n$ are linearly independent.
Proof: In a cyclic code, any cyclic shift of a codeword is another valid codeword. Hence right shifting each row of G j times, we get an upper triangular matrix in columns $\{j+1, j+2, \cdots, \jmath+k\}$ mod n. This submatrix has full rank. Hence, we can take any consecutive k bits as message bits.

4. (a) $n = 7$, $g(x) = 1 + x + x^3$. All codewords of the binary cyclic code is listed using the generator matrix

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Message bits $\underline{m}$	Codeword bits $\underline{c}$
0000	0000000
0001	0001101
0010	0011010
0011	0010111
0100	0110100
0101	0111001
0110	0101110
0111	0111001
1000	1100101
1001	1100101
1010	1110010
1011	1111111
1100	1011100
1101	1010001
1110	1000110
1111	1001011

Table 1: Codeword table.

(b) If $f(x)g(x) = 0$ in R_7 then $f(x)g(x) = a(x)(x^7+1)$. We know that $x^7 + 1 = g(x)h(x)$ with $\deg(h(x)) = 4$. Also, $\dfrac{f(x)g(x)}{x^7+1} = a(x)$.

$$\begin{aligned} x^7 + 1 &\mid f(x)g(x) \\ g(x)h(x) &\mid f(x)g(x) \\ h(x) &\mid f(x) \\ \implies f(x) &= a(x)h(x), \end{aligned}$$

where $a(x)$ is a polynomial of degree at most 2.

5. After simplification generator polynomial, $g(x) = x^8 + x^7 + x^6 + x^4 + 1$. A generator matrix is

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

The parity check polynomial is calculated as follows:

$$\begin{aligned} h(x) &= \frac{x^{15}+1}{x^8+x^7+x^6+x^4+1}, \\ &= x^7+x^6+x^4+1. \end{aligned}$$

The generator polynomial for the dual is

$$\begin{aligned} g^{\perp}(x) &= x^k h(x^{-1}), \\ &= 1+x+x^3+x^7. \end{aligned}$$

Therefore, a parity check matrix is

$$\mathbf{H} = \begin{bmatrix} 1&1&0&1&0&0&0&1&0&0&0&0&0&0&0 \\ 0&1&1&0&1&0&0&0&1&0&0&0&0&0&0 \\ 0&0&1&1&0&1&0&0&0&1&0&0&0&0&0 \\ 0&0&0&1&1&0&1&0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&1&0&1&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&1&0&1&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&1&0&1&0&0&0&1&0 \\ 0&0&0&0&0&0&0&1&1&0&1&0&0&0&1 \end{bmatrix}.$$

6. The generator polynomial of an (n,k) cyclic code is a degree-$(n-k)$ factor of x^n+1. Therefore, for a given block length n, we have many choices for message length k.

n	Size of cyclotomic cosets	Possible k
15	1,4,4,2,4	$1 \le k \le 15$
31	1,5,5,5,5,5,5	1,5,6,10,11,15,16,20,21,25,26,30,31
51	1,2,8,8,8,8,8,8	1,2,3,8,9,10,11,16,17,18,19, 24,25,26,27,32,33,34,35,40,41,42,43,48,49,50,51

Table 2: Possible dimensions for cyclic codes.

7. (a) A generator matrix for the code is

$$\mathbf{G} = \begin{bmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 1 \end{bmatrix}.$$

The codewords are listed in Table 3.

(b) Over $GF(4)$, x^3+1 factors into linear terms. Therefore,

$$x^3+1=(x+1)(x+\alpha)(x+\alpha^2).$$

Grouping the factors other than $g(x)$, we get the check polynomial as follows:

$$h(x)=x^2+\alpha x+\alpha^2.$$

The generator polynomial of $C^{\perp}$ is

$$\begin{aligned} g^{\perp}(x) &= x^k h(x^{-1}) \text{ scaled to be in monic form,} \\ &= \alpha^{-2}x^2 h(x^-1), \\ g^{\perp}(x) &= \alpha+\alpha^2 x+x^2. \end{aligned}$$

Message bits	Codeword Symbols over $GF(4)$	Code bits over GF(2)	Weight
00	000	000000	0
01	$0\alpha 1$	000110	2
0α	$0\alpha^2\alpha$	001101	3
$0\alpha^2$	$01\alpha^2$	001011	3
10	$\alpha 10$	011000	2
11	$\alpha\alpha^2 1$	011110	4
1α	$\alpha\alpha\alpha$	010101	3
$1\alpha^2$	$\alpha 0\alpha^2$	010001	2
$\alpha 0$	$\alpha^2\alpha 0$	110100	3
$\alpha 1$	$\alpha^2 01$	110010	3
$\alpha\alpha$	$\alpha^2 1\alpha$	111001	4
$\alpha\alpha^2$	$\alpha^2\alpha^2\alpha^2$	111111	6
$\alpha^2 0$	110	101000	2
$\alpha^2 1$	111	101010	3
$\alpha^2\alpha$	10α	100001	2
$\alpha^2\alpha^2$	$1\alpha\alpha^2$	100111	4

Table 3: Cyclic code over GF(4).

(c) We make use of the result in 8a. The other generator polynomials for which $x+\alpha$ is a factor are

$$\begin{aligned} g_1(x) &= (x+1)(x+\alpha) \\ &= x^2+\alpha^2 x+\alpha, \\ g_2(x) &= (x+\alpha)(x+\alpha^2) \\ &= x^2+x+1. \end{aligned}$$

Therefore, the cyclic codes which are contained in C are

$$\begin{aligned} C_1 &= < x^2+\alpha^2 x+\alpha >, \\ C_2 &= < x^2+x+1 > . \end{aligned}$$

8. (a) Suppose $C_1 \subseteq C_2$. Then, the generator polynomial $g_1(x) \in C_1 \subseteq C_2$. Hence, $g_1(x) \in C_2$, which can happen only if $g_2(x)|g_1(x)$. For the converse, suppose $g_2(x)|g_1(x)$. Let $c_1(x) \in C_1$. Then,

$$\begin{aligned} c_1(x) &= m(x)g_1(x), \\ &= m(x)a(x)g_2(x), \\ &= d(x)g_2(x) \in C_2. \end{aligned}$$

Therefore, $C_1 \subseteq C_2$.

(b) If $g_2(x)|g_1(x)$, the zeros of C_2 will be a subset of the zeros of C_1.

(c) Suppose Z is the set of zeros of C. The set of zeros of $C^\perp$ is $-Z^C \mod n$, where n is the blocklength and $Z^C = \{0,1,2,\cdots,n-1\} \setminus Z$. If $C \subseteq C^\perp$, then $-Z^C \mod n \subseteq Z$.

9. (a) Suppose the code is cyclic. Since $k=3$, we see that the first row of G will be the generator polynomial, or $g(x) = 1+x+x^2$. By Euclid's algorithm, $x^5+1 = (x^3+x^2+1)(x^2+x+1)+x$. Therefore, $g(x)$ does not divide x^5+1. Hence the code is not cyclic.

(b) Since the given matrix is a square matrix, we will first check whether the given matrix is full rank using Gauss Elimination.

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Generator matrix is a full rank matrix. Hence it is an identity code and cyclic.

(c) Since $k = 4$, the generator polynomial should be $g(x) = 1 + x + x^2$. We can check that

$$(x^2 + x + 1) \mid x^6 + 1 = (x^3 + 1)^2 = ((x + 1)(x^2 + x + 1))^2.$$

Therefore, $g(x)$ is a valid generator polynomial, and the code is cyclic.

10. If $g(x)$ is a valid generator polynomial then $g(x)|x^n + 1$. By Euclid's algorithm

$$x^{21} + 1 = (x^{11} + x^8 + x^7 + x^2 + 1)(x^{10} + x^7 + x^6 + x^4 + x^2 + 1).$$

Hence, $g(x)$ is a valid generator polynomial for a $(21, 11)$ cyclic code. Check polynomial for this code is $h(x) = x^{11} + x^8 + x^7 + x^2 + 1$.

11. (a) Let $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$. Since $x + 1$ is a factor of $g(x)$, $c(1) = 0$, or

$$c_0 + c_1 + \ldots\ldots + c_{n-1} = 0.$$

Since we are doing all operations over $GF(2)$, the above is possible only when the code contains even weight codewords.

(b) If $x+1$ is not a factor of $g(x)$, $x+1$ is a factor of the check polynomial $h(x)$ and the generator polynomial for the dual $x^k h(x^{-1})$. Therefore, all codewords of the dual code $C^\perp$ have even weight. Hence, C contains the all-1s codeword.

12. To check that $g^*(x) = x^{n-k}g(x^{-1})$ is a valid generator polynomial, we need to show that $g^*(x)$ divides $x^n + 1$. Now

$$\begin{aligned} g(x)h(x) &= x^n + 1, \\ g(x^{-1})h(x{-}1) &= x^{-n} + 1, \\ x^n g(x^{-1})h(x{-}1) &= x^n(x^{-n} + 1), \\ x^{n-k}g(x^{-1})x^k h(x{-}1) &= 1 + x^n, \\ g^*(x)h^*(x) &= 1 + x^n. \end{aligned}$$

Hence, $g^*(x)$ is a generator polynomial of a cyclic code C^*. Every codeword of C^* is a mirror-reflected version of a codeword of C. Hence, the minimum distance of C^* is d.

13. The ideal generated by the polynmial $f(x) = 1 + x + x^2 + x^4$ is

$$C = \{a(x)(1 + x + x^2 + x^4 \mid \ a(x) \in GF(2)[x]\ (x^5 + 1)\}.$$

Factoring $f(x)$ as $f(x) = (x + 1)(x^3 + x^2 + 1)$, we see that $x + 1$ is the only common factor of $f(x)$ with $x^5 + 1$. Hence, the generator polynomial of C is $x + 1$.

14. The answers are given in Table 4.

15. (a) $C^\perp$ is an even-weight code. Hence, the all-1s codeword belongs to C (since the all-1s vector is orthogonal to all codewords in $C^\perp$, the dual of C).

Code	Generator Polynomial	Parity Check Polynomial
$C =< g(x) >$	$g(x)$	$h(x)$
$C^{\perp} =< g(x) >^{\perp}$	$x^k h(x^{-1})$	$x^{n-k} g(x^{-1})$
$D =< h(x) >$	$h(x)$	$g(x)$
$D^{\perp} =< h(x) >^{\perp}$	$x^{n-k} g(x^{-1})$	$x^k h(x^{-1})$

Table 4: Code and its generator and check polynomial

(b) For a given cyclic codeword, all cyclic shifts of the codeword belong to the code. By right-shifiting the codeword [001111111111000] three times, we get [000001111111111] $\in C$. Since the code is linear, addition of two codewords will also be a codeword. Hence, we get a new codeword

$$\underline{c} = [111110000000000] = [000001111111111] + [111111111111111] \in C.$$

In polynomial notation, this new codeword is $c(x) = 1 + x + x^2 + x^3 + x^4$, which is the unique polynomial of degree 4 in the (15,11) cyclic code. Hence, the generator polynomial is $g(x) = 1 + x + x^2 + x^3 + x^4$.

(c) For a message polynomial $m(x) = x + 1$, the code polynomial $c(x) = (x + 1)g(x) = x^5 + 1$. Hence $d \leq 2$. We can rule out $d = 1$, since that will result in a dimension 15 identity code (why?). Hence, $d = 2$.